CLAIMS

1. A method for authenticating an imaging device operator's identity, comprising the steps of:

obtaining, from at least one biometric sensor, biometric information indicating said operator's identity;

capturing an image with said imaging device, substantially simultaneously with the step of obtaining said biometric information;

storing said biometric information together with said captured image;

wherein said identity of said operator is authenticated by said stored biometric information.

2. The method of Claim 1, wherein said at least one biometric sensor is selected from the group consisting of fingerprint sensors, finger sensors, palm sensors, iris sensors, retina sensors, eye sensors, and face sensors.

3. The method of Claim 1, wherein said at least one biometric sensor is selected from the group consisting of capacitance measurement based sensors, resistance measurement based sensors, optical measurement based sensors, and ultrasonic measurement based sensors.

4. The method of Claim 1, further comprising the step of:

analyzing said biometric information to create at least one biometric signature from said biometric information.

5. The method of Claim 4, further comprising the step of:

using said biometric signature to provide a reduced representation of said biometric information.

6. The method of Claim 1, wherein said imaging device is any of a digital imaging device and a recording film based imaging device.

7. The method of Claim 1, further comprising the steps of:

processing said biometric information and said captured image, prior to storing said biometric information and prior to storing said captured image.

8. The method of Claim 7, further comprising the step of:

subsequently verificating that said stored biometric information and said stored image have not been altered and have not been falsified.

9. The method of Claim 7, wherein said step of processing said biometric information and said captured image comprises computing a digital signature.

10. The method of Claim 9, wherein said digital signature is generated using a message digest.

11. The method of Claim 10, wherein said message digest is created using a hashing algorithm applied to said captured image and said biometric information.

12. The method of Claim 7, wherein said step of processing said biometric information and said captured image comprises the step of:

encrypting said captured image to produce an encrypted image.

13. A method for authenticating the identity of an operator of an imaging device, comprising the steps of:

retrieving an image captured by said image device;

retrieving biometric information that is associated with said image at substantially the same time that said image is captured;

obtaining candidate biometric information indicating the identity of a supposed operator of said imaging device;

comparing said candidate biometric information and said stored biometric information; and

authenticating said supposed operator as said imaging device operator at the time of capture of said image if said stored biometric information substantially matches said candidate biometric information.

14. The method of Claim 13, wherein said candidate biometric information is obtained directly from said supposed operator using a least one biometric sensor.

15. The method of Claim 13, wherein said candidate biometric information is obtained from a database of biometric information.

16. The method of Claim 13, wherein said imaging device is any of a digital imaging device and a recording film based imaging device.

17. The method of Claim 13, further comprising the step of:

verifying said stored biometric information and said stored image, after retrieving said stored biometric information, after retrieving said stored image, and prior to comparing said candidate biometric information and said stored biometric information to ensure that said stored biometric information and said stored image have not been altered and/or falsified.

18. The method of Claim 17, wherein said step of verifying said biometric information and said captured image comprises the step of:

verifying a digital signature.

19. A method for authenticating an imaging device operator's identity, comprising the steps of:

obtaining, from at least one biometric sensor, biometric information indicating said operator's identity;

capturing an image with said imaging device, substantially simultaneously with the step of obtaining said biometric information;

storing said biometric information, together with said captured image;

subsequently:

retrieving said image;

retrieving said biometric information;

obtaining candidate biometric information indicating the identity of a supposed operator of said imaging device;

comparing said candidate biometric information and said stored biometric information; and

authenticating said supposed operator as said imaging device operator at the time of capture of said image if said stored biometric information substantially matches said candidate biometric information.

20. The method of Claim 19, wherein said at least one biometric sensor is selected from the group consisting of fingerprint sensors, finger sensors, palm sensors, iris sensors, retina sensors, eye sensors, and face sensors.

21. The method of Claim 19, wherein said at least one biometric sensor is selected from the group consisting of capacitance measurement based sensors, resistance measurement based sensors, optical measurement based sensors, and ultrasonic measurement based sensors.

22. The method of Claim 19, further comprising the step of:

analyzing said biometric information to create at least one biometric signature from said biometric information.

23. The method of Claim 19, further comprising the step of:

using said biometric signature to provide a reduced representation of said biometric information.

24. The method of Claim 19, wherein said imaging device is any of a digital imaging device and a recording film based imaging device.

25. The method of Claim 19, further comprising the step of:

processing said biometric information and said captured image, prior

to storing said biometric information and prior to storing said captured image.

26. The method of Claim 25, further comprising the step of:

verifying said biometric information and said image, after retrieving said biometric information, after retrieving said image, and prior to comparing said candidate biometric information and said biometric information.

27. The method of Claim 26, wherein said processing step conditions said stored biometric information and said image for subsequent verification, and

wherein said verifying step ensures that said stored biometric information and said image have not been altered and/or falsified.

28. The method of Claim 26, wherein said processing step comprises:

computing a digital signature.

29. The method of Claim 26, wherein said verifying step comprises:

verifying said digital signature.

30. The method of Claim 29, wherein said digital signature is generated using a message digest.

31. The method of Claim 30, wherein said message digest is created using a hashing algorithm applied to said captured image and said biometric information.

32. The method of Claim 26, wherein said processing step comprises:

encrypting said captured image to produce an encrypted image.

33. An apparatus for authenticating an imaging device operator's identity comprising:

at least one biometric sensor for capturing biometric information indicative of said operator's identity;

recording device for capturing an image substantially simultaneously with said capture of biometic information; and

a medium for storing said biometric information together with said stored image for subsequent authentication of said operator's identity based on said stored biometric information.

34. The apparatus of Claim 33, wherein said at least one biometric sensor is selected from the group consisting of fingerprint sensors, finger sensors, palm sensors, iris sensors, and face sensors.

35. The apparatus of Claim 33, wherein said at least one biometric sensor is selected from the group consisting of capacitance measurement based sensors, resistance measurement based sensors, optical measurement based sensors, and ultrasonic measurement based sensors.

36. The apparatus of Claim 33, further comprising:

means for analyzing said biometric information to create at least one biometric signature form said biometric information.

37. The apparatus of Claim 33, further comprising:

means for generating a reduced representation of said biometric information.

38. The apparatus of Claim 33, wherein said imaging device is any of a digital imaging device and a recording film based imaging device.

39. The apparatus of Claim 33, further comprising:

a processor for processing said biometric information and said captured image, prior to storing said biometric information and prior to storing said captured image.

40. The apparatus of Claim 39, wherein said processor subsequently verifies that said stored biometric information and said image have not been altered and/or falsified.

41. The apparatus of Claim 39, wherein said processor computes a digital signature.

42. The apparatus of Claim 41, wherein said digital signature is generated using a message digest.

43. The apparatus of Claim 42, wherein said message digest is created using a hashing algorithm applied to said captured image and said biometric information.

44. The apparatus of Claim 39, wherein said processor encrypts said captured image to produce an encrypted image.